Vasyl Ustimenko (Institute of telecomunications and global information space, NAS, Kiev, Ukraine)

On Extremal Graph Theory for Directed Graphs and its Applications to Information Security

Classical Extremal Graph Theory developed by P. Erdös' and his school had been started with the following problem motivated by its applications to Telephone Networking:

The girth of the simple graph is the length of its smallest cycle. What is the maximal value $ex(v,n)$ for the size (number of edges) of graph on v vertices with the girth $> 2n$?

Notice that if the girth $> 2n$ then two vertices at the distance $\leq n$ are connected by the unique pass.

According to the well known Even Circuite Theorem $ex(v,n) \leq O(v^{1+1/n})$. This bound is known to be sharp for $n = 2, 3$ and 5 only.

The upper bound above and the first general lower bounds of kind $ex(v,n) \leq O(v^{1+1/(cn)})$, where c is some constant > 1 had been obtained in 50th by famous Erdös' probabilistic method.

Explicit constructions of families of graphs of large girth i.e. regular graphs of unbounded degree and girth such that their size is above $O(v^{1+1/(cn)})$ for some positive constant c appeared in early 90th. These results of algebraic nature allows to get the known smallest c, $c = 3/2$. Just few algebraic families of graphs of large girth are known.

It is known that finite automaton roughly is a directed graph with labels on arrows. So the Computer Science motivates the development of Extremal Graph Theory for Directed Graphs. We will consider here the directed graphs without loops and multiple arrows. We assume that the commutative diagram is formed by two directed passes for which the same starting and ending points form the full list of common vertices. We refer to the length of maximal pass (number of arrows) as the rank of the diagram. We will count a directed cycle of length m as a commutative diagram of rank m

Let us assume that the girth indicator gi, gi ≥ 2 of the directed graph is the minimal rank of its commutative diagram. Notice that if the girth indicator of the graph is $> d$, then for each pair of vertices a, b the number of directed passes from a to b of length $\leq d$ is ≤ 1.

Notice that studies of maximal size of directed graphs without certain commutative diagrams without some restrictions on numbers of inputs or outputs of the vertex do not make a sense. graph. Really, the graph with the vertex set: $P \cup L = V$, partited into point set P and line set L of same cardinality, $|P \cap L| = 0$, $|V|$ is even number v, formed by all arrows from point to line has order $O(v^2)$ and does not containe directed cycles or commutative diagrams. That is why we will consider only balanced graphs for which the number i_v of inputs $xrightarrowv$ and number o_v of outputs $v \rightarrow x$ are same for each vertex v.

Theorem 1 *Let $E(d,v)$ be the maximal size $E(d,v)$ (number of arrows) for the balanced graph on v vertices with the girth indicator $> d$. Then $E(d,v) = v^{1+1/d} + O(v)$.*

Remark 1. It is easy to see that the upper bound $ex(v,n) \leq O(v^{1+1/n})$ follows from the above theorem. But the questions on the sharpness of the bound for $n \neq 3,4$ and 6 are still open.

Remark 2. The inequality $E(d,v) \leq v^{1+1/d} + O(v)$ has been obtained by probabilistic arguments while the sharpness of this bound has been obtained via explicit constructions.

Directed graphs of large girth can be defined as regular graphs of unbounded degree and the girth indicator such that their size is close to the bound of the above statement. above $O(v^{1+1/(cn)})$ for some positive constant c appeared in early 90th. These results of algebraic nature allows to get the known smallest c, $c = 3/2$. Just few algebraic families of graphs of large girth are known.

The latest results on the applications of the graphs of large girth (simple or directed) and related discrete dynamical systems to the design of encryption algorithms and turbocoding the reader can find in [1]-[4].

[1] T. Shaska, W. C. Huffman, D. Joener and V. Ustimenko (editors), Advances in Coding Theory and Cryptography. — Series on Coding Theory and Cryptology, World Scientific, vol. 3, (2007): look at "On the extremal graph theory for directed graphs and its cryptographical applications" (V. Ustimenko).

[2] Roland E. Chen (editor), Cryptography Research Perspectives. — Nova Science Publishers - April 2009, see Chapters "On the Properties of Stream Ciphers Based on Extremal Directed Graphs" (V. Ustimenko and J. Kotorowicz) and "Private and Public Key Systems Using Graphs of High Girth" (A. Touzene and V.Ustimenko)

[3] Proceedings of the NATO Advanced Studies Institute "New challenges in digital communications". — May 2008, University of Vlora, Vlora, Albania, Special issue of Albanian Journal of Mathematics, 2008 v.2, issue 3, "On some applications of graph theory to cryptography and turbocoding" (T. Shaska and V.Ustimenko).

[4] T. Shaska, E. Hasimaj, Mathematics and Communications. — T. Shaska, E. Hasimaj, Mathematics and Communications, IOS Press, to appear in 2009 [Lectures of Advanced NATO Institute "New Challenges in Digital Communications, Vlora, 2008, see "On the cryptographical properties of extremal algebraic graphs" (V. Ustimenko)] IOS Press, to appear in 2009.